The Long Way from Electronic Traces to Electronic Evidence

Dinant, Jean-Marc

Published in:
International Review of Law Computers & Technology

Publication date:
2004

Document Version
Publisher's PDF, also known as Version of record

INTERNATIONAL REVIEW OF LAW COMPUTERS & TECHNOLOGY, VOLUME 18, NO. 2, PAGES 173–183, JULY 2004

Carfax Publishing
Taylor & Francis Group

The Long Way from Electronic Traces to Electronic Evidence

JEAN-MARC DINANT

ABSTRACT *Generally, traces of Internet communications established by a citizen's computer are routinely recorded on and dated by Internet servers in so-called 'log files'. As far as the correct dating of the electronic offence is crucial for the potential identification of the author, convincing traces need to be date- and time-stamped by a Trusted Third Party (TTP). Such a time stamp does not give any assurance about the correctness of the data and dates collected, but only proves that the traffic data were in a given state at a given date and time. If the Internet Provider (IP) address appears to be one used by the company, it is foreseeable that the system administrator within the company will be able to identify the computer owning a particular IP address. In others cases, only law enforcement agencies, in the circumstances and the conditions required by the law, are entitled to identify, with the help of Internet Access Providers (IAPs), the communication line suspected to have been used beside a given IP address. Putting together the traces left at the IAP side and in the log files of the attacked server site may lead, in the best cases, to an identified communication terminal. Nevertheless, in many cases, this will not be a formal authentication of a wrongdoer.*

Introduction

This paper aims to be a simple review of best practice tricks for handling, building, keeping and searching an evidence database and producing a technically valuable proof.

This paper focuses on the HTTP protocol, the most widely used protocol on the Internet on the top of the TCP/IP protocol. It does not pretend to embrace the full problematic of traces of exploitation on the Internet.

Because this paper is not only aimed at the computer scientist but is also aimed at those in small to medium sized enterprises (SMEs) with a basic knowledge of how a telecommunication network works, a short introduction describes the axioms of the Internet and the

Correspondence: Jean-Marc Dinant, Centre de Recherches Informatique et Droit, 5 Rempart de la Vierge, 5000 Namur, Belgium. E-mail: jean-marc.dinant@fundp.ac.be

ISSN 1360-0869 print/ISSN 1364-6885 online/04/020173-11 © 2004 Taylor & Francis Ltd
DOI: 10.1080/1360086042000223490

traces that a netizen produces when surfing on the Internet. A particular emphasis is made on the kind of actors routinely collecting those traces, in the running phase. This paper does not deal with the legal compliance of the collection, storage and transmission of traces. Depending on the kind of actors collecting or 'owning'[1] the data, distinct laws apply. This paper concentrates on the convincing character of data collected taking into account the state of the art in both computer security and computer attacks.

The author of this paper benefits from a modest personal experience of being an 'expert witness'[2] before many civil courts in Belgium, and as an individual, cannot always perfectly dissociate his personal practice and history from the theory, but does not want to generalise or extrapolate his own practice in a global theory. As a member of a multidisciplinary centre of research dealing with law and computer science, the author has always tried to be a gateway between the law and the technology and vice-versa.

An original tool has been developed within the CTOSE project that permits one to see both online and in real time[3] the actual logfiles of the Web server hosting the www.ctose.org. For confidentiality reasons, the exact URL will not appear in this version of this paper. Within the WP3 team, this page has been extensively used to show very clearly to lawyers the traces that are routinely collected by a standard web server, and how it is possible to find and to exploit the traces left by an attack.

While trying to turn some traces into valuable evidence, one determining key issue is to demonstrate the exact date and time of the attack. Two methods are possible.

(1) The traditional one and that consists of an official act posed by an official institution such as the police, or one bailiff,[4] who will testimony a fact or certify the existence of a given document such as a logfile at a determined time.
(2) A modern method based on the signature by a Trusted Third Party (TTP) of an electronic document such as a logfile. The IETF has developed such a protocol,[5] which is at the 'proposed standard' state.

We will examine the advantages of using both traditional and electronic methods.

Traces on the Internet: Who Collects What?

There are several relevant kinds of actors involved in an Internet[6] communication.

(1) the netizen who will visit a website;
(2) the Internet Access Provider of the netizen;
(3) the Internet Service Provider of the Website

Traces at the Netizen Side

This paper will not detail the traces left on the computer of a surfer. One the one hand, a naive web surfer will typically leave many traces on the navigator cache installed on his hard disk drive. On the other hand, a malicious intruder with a technical background will probably use others tools[7] that will directly access the IP network without any caching mechanisms.

In the first case, the data downloaded from the network on the netizen PC will remain accessible over a period of a few weeks. A computer expert can very easily discover those traces if the forensic process takes place a short period after the offence.

In the second case, the information downloaded will probably not be so easy to find. The discovery of a tool permitting a possible offender to produce self-made HTTP requests is

not necessarily a proof of illegal behaviour. A forensic approach will probably be necessary to find reliable proof of evidence

Traces Common Collected by the Internet Access Provider

On the basis of a nominative contract,[8] the IAP provides a TCP/IP connectivity to individuals using a modem(analog or ADSL) or a terminal adapter (ISDN). In this case the subscriber will receive an IP address for the duration of his/her connection and this address will probably change the next time he/she dials up. This is called a dynamic IP address. In the case of a connection within the intranet of a company, the IP address can be either static or dynamic by using the DHCP protocol. Even for a dynamic ADSL connection, it seems that many IAPs frequently changed their own IP address (typically every 24 hour), and therefore an Internet IP address need not necessarily be permanently linked to a particular individual.

It should be noted that it is a standard practice for an IAP to collect the detail of the IP addresses given to a particular customer for a determined amount of time in a log file. This means that an IAP can easily, at least over a certain period,[9] find a customer by having their IP address and the exact date of the usage of this IP. Because IAPs are not law enforcement agencies, the netizen can always get access to his own data during the retention time. Furthermore, because IP addresses linked with a customer ID are personal data, they may not disclose the identity of a netizen to a third party unless required to do so by a judge or by a law enforcement agency under the conditions written in a law.

It has to be underlined that contrary to popular opinion the IAP does not routinely collect the IP addresses of the website visited by their customers. Nor do they by default[10] (unless the law requires them to do so) collect any details of the electronic transactions made on those websites. The IAP can be regarded as a telecommunication operator such as BT or France Telecom. Unlike a telephone company, an IAP is normally[11] unable to know, on a one to one basis, the number called by the subscriber. What is routinely collected has to be checked.

Organisations use a dialup connection or, more often, a line leased to the company's office. The traditional telecom operator will normally provide this leased line. The connection can also be established via a satellite line or a terrestrial radio system. The IAP will usually give IP addresses (a 'class') to the company as a whole and install a router at both ends of the line. In most cases, this router will normally avoid illegal IP addresses when sending IP packets to the outside world.[12] Within the company, the IP addresses are distributed:

- Manually, on a case by case basis. This means that the IT manager will assign one static IP address to each computer.
- Automatically, by using a so-called DHCP[13] server internal to the organization that will assign one IP address (among the class hired to the IAP) when the computer starts. These DHCP servers are able to keep track of the IP given to distinct computers identified by their MAC address[14] in a log file.

Therefore, the IT manager will generally be able to link an IP address owned by the company to the computer that was using this IP address during a particular period of time. Of course, this remains true only during the retention of the data stored in the logfiles.

As a conclusion, generally speaking, an IP address may easily be linked to a physical person by the IAP who has 'hired' this address or by a company well known by this IAP. This may not be the case if the netizen is using an anonymous communication line

(cybercafé or a pool of computers within a university or a library) or is using anonymising relays like IP masquerade at the IP level[15] or an HTTP proxy server so hiding the address of the client.[16] Wireless connections constitute a major challenge here as far as there is no physical link between a potential intruder and the local area network (LAN) of a company. In this case, electronic traces will probably, in the best case, consist of the serial number of the wireless card and will lead to nobody unless this card is retrieved.

The Internet Service Provider

The Internet Service Provider provides services to the Internet as a whole, namely by permanently connecting Web servers on the Internet. Many other types of servers can be deployed, such as SMTP servers (for mail relay), FTP servers, NNTP servers, etc.

In many cases, the company can be their own Internet Service Provider and host their website on their own computer, linked to the Internet thanks to an IAP.

Very commonly, HTTP servers are by default configured to generate logfiles. What can be found on those log files? A relevant example may be found on the CTOSE web server. The CTOSE web server hosts on www.ctose.org both the Intranet and the Extranet of the CTOSE project. It consists of a dedicated computer linked to the Internet running an Apache[17] Web Server on a Windows NT4 server. Apache is a robust and free HTTP server running on various operating systems (OS) (Windows 95/98/NT/2000, Linux, Unix, etc) and is considered as a standard in itself. Its main competitor is the Microsoft Internet Information Server (Microsoft IIS)

The data collected and written down by the Apache Server, just like other Web servers, may be classified into three categories:

(1) Data related to the IP level (namely the DNS[18])
(2) Data transmitted by the web browser itself. These data are called 'browser's chattering',[19] just because they include many data that are not useful for permitting an efficient communication between a Web server and a visitor but are widely used to profile and track the netizen. These data are:[20]
   - Kind of computer used
   - Exact version of the OS installed
   - Language of the OS
   - Type and version number of the browser used
   - Type of content readable by the browser
   - Language references of the netizen
   - Cookies
   - Referring page[21]
(3) Data generated by the web server itself
   - The URL of the document asked
   - The status code[22]
   - The number of bytes actually sent as a response to the request
   - The exact date and time when satisfying the request. It is important to note that the server computer internal clock generates these dates and times. Such clocks are not very precise and, furthermore, it is possible that a malicious intruder could gain sufficient right to modify the exact hour *before* the attack and restore the exact time *after* the attack[23]
   - The user ID if authentication was required

Four sample extracts issued from the CTOSE logfiles are described below.

The first one is normal and is not an attack.

213.223.66.60	[the IP address of the visitor. By issuing a reverse DNS cheek (e.g. *ping -a 213.223.66.60 in a command line window*) we can see that the DNS of the IP is ceg-netc.alcatel.fr. This is absolutely nirmal as far as Alcatel is a partner of the Ctose project.
200	Status OK : the web page has been found and delivered
2002/08/27	Date of the request
18:07:13	Time of the request
ctose	Name of the authenticated user
GET /intranet/list.html	URL of document asked
HTTP/1.	Kind and version of the protocol used
5094	Number of bytes transferred
http://www.ctose.org/intranet/	Referring page
Mozilla/4.79 [en]	Means Netscape Communicator version 4.79
(Windows NT 5.0; U)	OS of the visitor is Windows NT 5.0, i.e. XP

The second one is the trace of an 'unsuccessful' attack.

217.231.205.76	IP address of the user
2002/07/10	Date of the user
14:53:21	Time of the user
-	User is not authenticated and nor identified
GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\\	User is obviously trying to execute a shell command in a directory named "script". This shell command tries to get the list of files and directories present on the root disk of the web server. This kind of security hole is not present on Apache.
HTTP/1.1	Kind and version of protocol used
404	Error Code : page has not been found
243	Bytes sent to the user (probably an error code)
	The attacker hide his browser brand and his OS

The third line is the trace left by the indexing robot of Google itself.

216.239.46.236	IP address used by Google indexing robot
2002/08/21	Date
00:05:37	Time
-	User not authenticated nor identified
GET /robots.txt	Google is searching for the file "robot.txt". When existing, this file describes what can be indexed and what search engines cannot report.
HTTP/1.0	Kind and version of protocol used
404	Status code. All the Ctose website can be indexed
204	Length of the reply of the CTOSE server (error)
-	Not a browser
Googlebot/2.1 (+http://www.googlebot.com/bot.html)	Referencing of Google indexing robot

The fourth sample line shows the traces left by somebody searching the *keywords* 'tools for investigators' by using Google as a search engine. This demonstrates that the indexing done by Google is efficient.

167.1.124.100	IP address of the visitor
2002/08/22	Date
02:49:46	Time
-	User not authenticated nor identified
GET /	Get the default document
HTTP/1.1	Kind and version of protocol used
200	Status OK. Page was found
3531	Size of the content transmitted
http://google.yahoo.com/bin/query?p=tools+for+investigators&b=61&hc=0&hs=6&xargs=0	Referring page : The user cames from the result page of Yahoo and was searching for "tools for investigators"
Mozilla/4.0 (compatible; MSIE 5.5;	Visitor is using Internet Explorer 5.5
Windows NT 4.0)	On an NT 4.0 computer

Conclusion

Between a netizen and a web site, there is always an IAP who will give an IP address to the netizen. Without an IP address, access to the Internet is impossible and in this way the IAP can be compared to a car rental company. The car rental company hires cars to citizens and knows normally who they are. On the basis of a plate number, they will be able, for a certain period, to trace the identity of a particular driver. By default, the car rental company does not know what has been done with the vehicle that has been rented.

At the other end, a company that is the victim of an incident will, in several cases, be able to note the plate number of the car used by the author of the incident. Unless the plate number relates to one of the vehicles used by the company, he will probably be unable to identify the driver of the vehicle. The company knows which car has been used to perpetrate the incident but it is unable to identify the author of the incident. It will be up to law enforcement agencies, conforming with the relevant legal requirements, to check the two sources of information in order to be able to describe who has done what.

As in the real world, tracing the IP address and identifying the subscriber of a contract will not always lead to the actual author. The car may be stolen, used behind the back of the subscriber (identity theft) or be equipped with false plates. The same problem exists in the virtual world.

From E-traces Back to the Culprit: Proof of the Identity of the Author of the Offence

When seeing an IP address in a logfile it is easily possible to identify the company 'owning' this address, simply by using tools available for free on the net to accomplish a search.[24] In the case of our first sample line, the response looks like:

```
domain:   alcatel.fr
descr:    ALCANET International
descr:    2 rue de la Baume
descr:    75008 Paris
```


ALCANET International is a company that is normally able to identify the person behind the domain name ceg-netc3.alcatel.fr. This kind of very simple search may currently lead to an IAP rather than a company. This means that the victim of an attack, who has the IP address of the intruder is able in almost every case to identify very easily a third party that would be able to identify the intruder.

Of course, many hackers are perfectly aware of the methodology described above and will use various subterfuges to avoid such identification. Experimental hackers will first try to identify a target with a very low degree of protection and then use this hacked computer to issue the actual attack. They may also use a chain of IP relays in various countries or continents. In this particular case, one innocent computer is being used as a relay, of course without the prior knowledge and/or consent of the owner of the computer.[25] Universities are favourite targets because, generally speaking, the level of security is not as high as the security in place in banks.

Contrary to what happens when filming a car committing an infringement (the driver will probably also be on the image), it remains difficult to be able to prove who has been the author of an electronic offence. This is especially true in the cases where a forensic analysis of the computer used to commit the attack is not possible or is inefficient, notably because the forensic process takes place too long after the electronic offence.

Time Stamping of Electronic Traces

During the suspicion and the investigation phase, it appears primordial to prove or to remain able to prove not only the identity of the intruder (or at least his IP address) but also the exact date and time of the attack.

Two Kinds of Date and Time Stamping

The time stamping performed by an individual. This is the classic form of time stamping. An individual (police officer, bailliff, etc.) will certify the trace, where existing, at a particular date and time. They can put a stamp on a paper document plus their signature. Just because logfiles consist of many thousand lines, they may be hard to time stamp by using a printed version. An easy way to solve this problem is to write the logfiles on a WORM[26] support that will then be manually signed and time stamped.

Time stamping protocols and public key infrastructure generalities. The principle of a time stamping protocol is to permit to a TTP to sign electronically a content with certification of the exact date and time of the signature. Within a Public Key Infrastructure (PKI), a signature is nothing more than a computation using a public algorithm and a secret number (key) applied to a particular digital content. In a PKI, keys are generated in couples and the axiom of a PKI is that what has been encrypted with a key can only be decrypted with the other key of the same pair. This is called asymmetric cryptography.

Alternatively, in a symmetric cryptography scheme, the same key is used both to crypt and to decrypt, as in real life.

The third category of cryptographic functions is the hashing function. A hashing function uses no key at all and a public algorithm. When applied to digital content, they produce a 'digest', similar to a digital fingerprint of a binary content. Whatever the size of

the original document, the digest will be relatively small (less than 1 Kbits). Even when many hundreds of thousand documents can theoretically have the same digest, it has been demonstrated that the finding of two documents having the same digest remains highly unlikely, even with very high computing power.

The speed of computation of asymmetric functions is extremely low, compared to symmetric function. This speed is linearly dependent on the size of the content to which the signature has to be applied. This is the main reason why the signature is almost never applied to the original content but to a small digest of the document. This encrypted digest is the signature of the document.

It remains very easy to demonstrate that a particular document signed by a TTP, without any kind of assistance of this particular TTP can:

(A) Apply the public key of the TTP to the digest and get the decrypted digest
(B) Apply the hashing function to the document that has been signed

If the number computed in (A) matches the number computed in (B) the signature is valid.

Systematic Time Stamping of Logfiles During the Normal Running State

By an individual. It is not conceivable to operate individual time stamping after each electronic communication. A possible solution is to timestamp the logfiles once a month. The problem is that in a normal state law enforcement agencies do not have any valid reason to conduct such a time stamping. However, it remains possible to ask to a bailiff to conduct such a certification but it is very unlikely that companies and notably SMEs will invest a single Euro for such a warranty.

Furthermore, this time stamping may, in many cases, be a very bad idea. It has been asserted by several IT managers during the interviews that a professional hacker will first delete all his traces in the logfiles just after being able to surreptitiously log in to a computer ... and probably also delete the traces of the modifications done to the logfiles. If this is the case, it is very unlikely that a monthly or a weekly and even a daily time stamping will happen between the intrusion and the erasing of the traces of the offence in the logfiles. Unfortunately, these logfiles that replace the traces of the malicious offence of a hacker will store the falsified traces of an innocent victim.

The date and time appearing in the logfile are not necessarily correct, due to two distinct reasons:

(1) The computer clock is not safe and/or precise and a low battery will generally cause this.
(2) It is possible that one substantial part of an attack is to change the computer time.

Electronic time stamping. One can argue that, thanks to TSPs, it is now very easy, technically speaking, to perform the time stamping of various data.

In correlation with what has been previously described, the TTP will date and time stamp not the log file itself but a digest of it.[27] The time for computing this digest is linearly dependent on the size of the logfile that needs to be loaded in the RAM memory. The time spent on conducting the computing of the digest may very soon appear prohibitive, especially in cases where performance is crucial. Furthermore, it is necessary to send the digest to the TTP after each transaction and this TTP will not offer a certified time stamp for free.

All these reasons lead to the conclusion that the time stamping of logs files by a TTP in the running phase is both inefficient and unrealistic in the normal running state of an information system.

The WP2 describes a technical alternative, namely the use of a dedicated computer operating inside the organisation offering certified date and time stamping.

Time Stamping During Suspicion and Investigation Phase

When entering the suspicion phase, it is necessary to freeze the data collected in such a way that they can not be altered even in good faith by the IT administrator or by the police.

This is the first thing to do and a good strategy is for the system administrator to be prepared to use the right freezing tools. It is therefore necessary to be able to provide at every moment a carbon copy of the existing data at the very beginning of an attack, when suspicion is rising. Just like a fire extinguisher, these tools need to be ready, in a perfect running state. The IT staff must be *a priori* trained in the use of such tools

When entering into the suspicion phase, it is necessary to work on a copy of the copy taken during the suspicion phase, unless the original copy has been performed on a WORM support. It very often happens that even the computer security experts change the data that they are analysing. If this is the case, it is not always possible to take another clean copy of the traces collected. In several cases, it can happen that, during the suspicion phase, a possible intruder is busy destroying all the traces left by his intrusion and this means that they will be impossible to find.

During the suspicion phase it is important to work on a copy of the traces left and never on the original.

Furthermore, the accused person also has the right to ask for an expertise of the data to prove his innocence. The same principle exists when seizing actual items.

It has to be noticed that the role of a computer expert remains essential to guarantee that this fundamental principle remains untouched. The 'Best practices for seizing electronic evidence'[28] instruction's recommends asking the assistance of a computer expert whenever a computer to be investigated is turned on. The role of this computer expert is not only to investigate the electronic traces to find evidence but also, *prima facie*, to freeze the traces collected in such a way that a contradictory analysis will be possible by the defence of the suspected person.

Conclusion

For producing valuable electronic evidence, it appears necessary to enhance the security of the electronic evidence processing itself. Generally speaking, in the best world, e-traces will be stored on a dedicated computer, on a transaction basis. A special emphasis must be put on a secure time stamping of e-traces, ideally by a trusted third party relying on a certified time source.

If those guarantees are met, there is a substantial probability of having some traces leading to a computer (this is the best case—e-traces may lead to no computer at all). However, such traces are rather useful in providing the identification of a possible intruder. In substance, because they are just a bit copy of original bits, they are rarely able to authenticate the author of an attack. This will not constitute a problem if the suspected person does not deny the facts or if there are non-technical suspicions about him.

However, if there is an identified suspect but this person denies authorship, all e-traces remain weak. Such e-traces are usually unable to prove who was behind the keyboard (this would require a biometric authentication), and furthermore, unable to prove that the person behind the keyboard at the time of the attack was knowingly hacking a network (perhaps his computer had been hacked by a third person using a Trojan horse). This last remark is due to the fact that the honest user is often unaware about what is happening on their computer. Finally, is it not this operating system opacity that creates the worst insecurity? When will cybercrime treaties apply to insecure software producers?

Notes and References

1 From a legal view, the data controller is not the 'owner' of the data.
2 'Expert judiciaire'.
3 The HTTP request made to get this logfile will, of course, not appear in this logfile, because the status of a transaction can only be written in a logfile by the HTTP server when the transaction has been completed (or aborted).
4 'Huissier de justice' in Belgium.
5 Internet X.509 Public Key Infrastructure Time-Stamp Protocol. In this document, we will use the term TSP. This protocol can be downloaded on http://www.ietf.org/rfc/rfc3161.txt?number = 3161.
6 Within this paper, the wording 'Internet' means the use of an IP network linked to the world and embraces both the Intranet as well as the Internet. This remark is important when knowing that a substantial number of electronic offences originate from the local networks of companies.
7 Typically, hackers will run a Telnet session with malicious scripts on a Unix/Linux computer or use a character-based browser like Lynx or Wget.
8 In order to obtain a connection, the individual has to conclude a contract and give his/her name, address and other personal data. Typically the user will receive a user identification name (UserId that may be a pseudonym) and a password so that nobody else can use his/her subscription. The authentication process during this subscription on line is usually very weak, i.e. the subscriber can give a false name and a false address. The use of the telecommunication line leaves traces at the telecommunication operator side, which are always linked to a particular phone line (unless in the context of a mobile phone functioning with an anonymous prepaid card).
9 Of course the duration of this period is at the heart of a debate between privacy advocates and law enforcement agencies. It seems that the legal delay may range from thee months to a year of two.
10 Just after having written this sentence, I have learned, by using personal and confidential contacts, that some IAPs are in fact storing the IP addresses contacted and the protocol used.
11 See note 7.
12 That is the best practice. Unfortunately, it has to be underlined that the IAP has no concrete interest for doing so. On the one hand, if an IP packet with a forged IP address escapes from their network, they may be quite sure that the police will not be able to find the origin of the packet. On the other hand, a machine issuing such a kind of packets will not cause a harmful damage to the IAP's network.
13 Dynamic Host Configuration Protocol. IP addresses may be attributed on a first come, first served, basis or on the basis of the MAC address, i.e. a serial number of the Ethernet LAN card that is sent in the header of each Ethernet packet on the LAN. This serial number is normally not routed outside a LAN.
14 The Medium Access Control number is a serial number unique at the world level that is transmitted in the Ethernet frames. Ethernet is the standard, low-level protocol widely used to set-up LANs.
15 Namely anonymizing services like www.zeroknowledge.com.

16 By default, many proxy servers add the field 'VIA' followed by the IP address in the HTTP header of the request. This is done for compliance with point 14.45 of the HTTP 1.1 specification, as published by the W3C. (see http://www.w3.org/Protocols/rfc2616/rfc2616.txt). Of course, normally, anonymous HTTP-Proxies will not send such data.
17 A robust, free web server downloadable on http://httpd.apache.org.
18 While the IP address is directly recordable, the corresponding domain name of the visitor is not sent during an HTTP communication. It is possible for a web server to do a reverse DNS search but it is widely inadvisable to execute automatically such a search because this kind of request needs an important amount of resources from the network as a whole to be satisfied. See the notice in the configuration file of Apache 'HostnameLookups Off; the default is off because it'd be overall better for the net if people had to knowingly turn this feature on, since enabling it means that each client request will result in AT LEAST one lookup request to the name server'.
19 A full view of what a browser is chattering can be viewed on a web page that the author has written: http://www.droit.fundp.ac.be/crid/privacy/WhatIknow.htm. It can be life tested by the reader of this document. A similar tool has been developed by the CNIL in France (http://www.cnil.fr/traces/index.htm).
20 Slight differences can be found among various browsers. In some cases, depending on the browser brand version and type, the browser chattering can be minimised by the user.
21 The exact URL where the netizen has just clicked in order to download the current page. The URL generally contents the keywords typed on a search engine if the current page has been found using a search engine.
22 Part of HTTP protocol (http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html). Code 200 OK means that the page has been found and correctly sent. Code 404 means that the page has not been found, etc.
23 This is a reason why a time stamping by an TTP can be appreciated.
24 http://www.ripe.net/perl/whois.
25 This is not only the personal opinion of the author but also the opinion expressed during two interviews conducted by CTOSE.
26 'Write Once, Read Many'. Typically it will be a non-rewritable CD-ROM (CD-R type).
27 As specified in the TSP developped by the IETF cited below (http://www.ietf.org/rfc/rfc3161.txt?number = 3161, Point 2.1.6 and 2.1.7): 'The Time Stamping Authority is required to only time-stamp a hash representation of the datum, ie a data imprint associated with a one-way collision resistant hash-function uniquely identified by an OID. (note of the Author OID = Object IDentifier) to examine the OID of the one-way collision resistant hash-function and to verify that the hash value length is consistent with the hash algorithm'.
28 A joint project of the International Association of Chiefs of Police and the United States Secret Service available on http://www.secretservice.gov/electronic_evidence.shtml.